Characterization and Analysis of NTP Amplification Based DDoS Attacks

L. Rudman
Department of Computer Science
Rhodes University
Grahamstown
g11r0252@campus.ru.ac.za

B. Irwin
Department of Computer Science
Rhodes University
Grahamstown
b.irwin@ru.ac.za

Abstract— **Network Time Protocol based DDoS attacks saw a lot of popularity throughout 2014. This paper shows the characterization and analysis of two large datasets containing packets from NTP based DDoS attacks captured in South Africa. Using a series of Python based tools, the dataset is analysed according to specific parts of the packet headers. These include the source IP address and Time-to-live (TTL) values. The analysis found the top source addresses and looked at the TTL values observed for each address. These TTL values can be used to calculate the probable operating system or DDoS attack tool used by an attacker. We found that each TTL value seen for an address can indicate the number of hosts attacking the address or indicate minor routing changes. The Time-to-Live values, as a whole, are then analysed to find the total number used throughout each attack. The most frequent TTL values are then found and show that the migratory of them indicate the attackers are using an initial TTL of 255. This value can indicate the use of a certain DDoS tool that creates packets with that exact initial TTL. The TTL values are then put into groups that can show the number of IP addresses a group of hosts are targeting.**

Keywords-component; denial of service; network security; network time protocol

I. INTRODUCTION

Distributed Reflection Denial of Service (DRDoS) attacks using Network Time Protocol (NTP) servers gained popularity in late 2013 and have been a factor in a number of major attacks in the first half of 2014. The Network Time Protocol is used to distribute accurate time information to networked computers. There are many public NTP servers throughout the Internet that are used by legitimate client systems in order to synchronize system clocks.

A NTP server which is exploitable in this type of attack allows the use of the 'MONLIST' command. This command returns up to the last 600 client IP addresses that have connected to an NTP server. Vulnerable NTP servers can thus provide a high degree of amplification scale as the MONLIST request packet is significantly smaller than the reply packet(s) generated. The MONLIST request UDP packet size is around 64 bytes and the reply "can be magnified to 100 responses of 482 bytes each" [7]. Combined with the ease of spoofing the source of UDP traffic, this amplification, makes NTP servers an ideal resource for DDoS attacks [3]. As seen in Figure 1, the attack is carried out by sending UDP/123 MONLIST request with a spoofed source address of the intended target of the attack to a vulnerable NTP server [8]. The server then sends the replies to the spoofed IP address (the victim) and are then flooded with large packets.

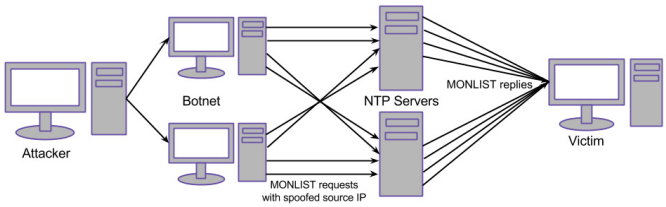

Figure 1. Distributed Denial of Service attack using NTP servers as reflectors.

In [8], it was stated that from January to February of 2014, the number of NTP amplification attacks had increased considerably with one of these attacks reaching just below 400 Gbps. They reported it as being the "largest attack recorded using NTP". By April 2014, Arbor Networks released data that showed that 85% of DDoS attacks above 100 Gbps were using NTP amplification [4]. In early 2014 there were more than 430,000 vulnerable NTP servers [4]. However by June 2014, this number decreased to around 17,647 vulnerable servers largely due to the application of patches and configuration changes by network administrators [7]. A report released by Arbor Networks in October 2014 showed that NTP amplification based attacks are decreasing, compared to April's data with a little over 50% of incidents in excess of 100Gbps using this protocol [6].

The problem with this class of attacks is that the real address of an attacker is never used due to the spoofing of the source IP address. As such more detailed analysis of such attacks is important in order to gain information which may be valuable in mitigating or finding the source of an attack. In this paper a number of characteristics of the attacks are looked at. The primary focus however relates to the observed TTL values within the IP header. The analysis of these has shown that they can be used to provide insight how many hosts are being used to generate request packets or where they may be in the world.

The remainder of this paper is structured as follows. Section II looks at related research in the area of Denial of service and NTP based Denial of service attacks in particular. The data sources used and analysis process undertaken are described in Section III. Results of the analysis of the two datasets are presented in Sections IV and V respectively. The paper

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

concludes with Section VI which also considers possible future work.

II. Related Work

As reported by Czyz et al. [2], NTP DDoS attacks were attacks were analyzed on a global scale by looking at the rise of NTP amplification attacks and how many amplifiers there are and their amplification scale. The victims of the attacks were found by looking at the source port of the original attack packet. And it was found that most of the victims were game related, with victims including *Minecraft*, *Runescape* and *Microsoft Xbox live*. The most popular source port found was port 80/udp, which they said may have been used to target games using this port or websites. When classifying the number attacks that occurred throughout a 15 week period monitoring a number of amplifiers, a simplification was used but classifying each unique targeted IP in a week long sample as one attack. This simplification does not take account of attacks targeting network blocks or a single IP hosting multiple sites.

In relation to TTL analysis it was determined in [2] that most of the attack traffic from a Colorado State University dataset appeared to originate from Windows-based machines and that they are probably botnet computers. This is because the mode of the IPv4 TTL field was observed to be 109, with the view that the default initial TTL set on Microsoft Windows platforms is 128. What these researchers failed to mention was that the attackers could have been using a DDoS tool that could have set the initial TTL to 128 or slightly above.

III. Research

Since at the time of the research being conducted in early 2014, there had not been much in depth research into the interplay of TTL values and NTP DDoS, the driver behind this research was to investigate a number of packet characteristics relating to the observed TTL values of recorded inbound traffic. In addition, the source IP address, source port, UDP header size and IP datagram size were also analyzed. The purpose of this was to determine the victims of the attacks in a similar manner to that used in [2].

A. Data Sources

The analysis carried out and presented in the remainder of this paper was based on two packet captures obtained from systems running a vulnerable version of the NTP software. Packet captures were recorded using tcpdump. The packet sizes were chosen to find the sizes of the MONLIST request packets going to the server, as most of the captured packets being analyzed were captured before the traffic was reflected. Any packet that did not contain a destination port of 123 was filtered prior to analysis out as they did not contain a MONLIST request, and would not have reached the vulnerable NTP servers for amplification. Both datasets were collected within South African IPv4 address space, contained within AS2018 (TENET).

The ZA1 data set consists of data collected between 15 July 2013 and 9 March 2014. The capture files have a combined size of 3.2 GB and contain a total of 32 799 299 packets. The captures show two attacks lasting around two weeks each. These were observed in the periods 23 December 2013 to 7 January 2014 and 10-25 February 2014 respectively. This dataset is of interest as the data capture was initiated pre-exploitation, and contains traffic destined for a single IP address.

The capture files constituting the ZA2 dataset consisted of 103 060 564 packets in total 11.5 GB, which were captured over a period of just over 1 month, from 12 February 2014 to 10 March 2014. This data was captured after the initially detected attack had been mitigated, but sees a larger number of packets per hour compared to ZA1. This is partially due to the fact that it was collected by recording traffic for the majority of target IP addresses within a single /27 IPv4 net block. For the purposes of this paper, the analysis across addresses has been merged, and individual activity has not been analyzed.

B. Analysis Tools

Analysis was performed using a series of custom based tools which were developed in python. This toolchain was used to parse and extract data form the raw packet captures, and then filter and plot time series graphs of information such as packets per hour, unique hosts per hour, IP addresses with a certain TTL, TTL per hour, IP datagram length, UDP datagram length, TTL frequency and others. The tools also outputted .csv files of the ranked source data which could be used for processing and analysis of the data in other tools.

IV. ZA1 Analysis

This section presents results of the analysis conducted on the ZA1 dataset. Two periods of exploitation were observed throughout 23 December 2013 to 7 January 2014 and 10-25 February 2014, these can be seen in Figure 2.

Peak packet rates in excess of 500 000 packets/ hour were observed in the initial attack. Packet rates packets subsequently decreased to around 50 000 packets/hour for the remainder of the attack. Significant diurnal trends were observed in the second phase. These patterns can be similarly observed in Figure 3 which plots the number of unique source hosts observed during each hour period. For both attacks the unique hosts started off with a considerably higher value than the rest of the unique host values of the attack. This is possibly due to attackers 'priming' the NTP servers, as in order to get the maximum amplification scale for the attack using the NTP MONLIST command, there must have been over 600 historical connections to the server, which can then be sent in response to the forged packet. The remainder of the section considers specific attributes of the observed attack traffic.

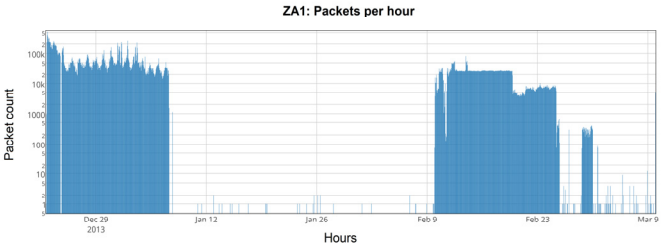

Figure 2. Packets per hour for ZA1

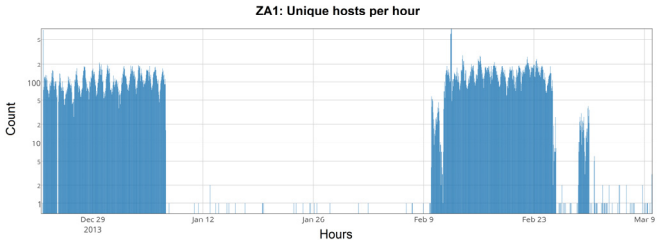

Figure 3. Unique hosts per hour

TABLE I. TOP 10 IP ADDRESSES FROM ZA1

Rank	*IP address*	*Count*	*% of total*	*TTL*
1	217.168.137.25	3,896,074	11.88	46 (9.21%) 47 (1.85%) 50 (88.54%)
2	72.46.150.210	320,816	0.98	
3	64.37.171.32	257,066	0.78	111
4	85.17.207.236	253,588	0.77	111
5	159.153.228.77	228,753	0.70	111
6	62.67.0.130	204,174	0.62	111
7	192.95.11.54	189,224	0.58	111
8	63.251.20.99	163,830	0.50	111 (98.73%) 232 (0.25%) 234 (1.20%)
9	212.143.95.26	154,368	0.47	111
10	75.126.29.106	150,659	0.46	111
	Total	5,818,552	% of total	17.74%

TABLE II. TOP 10 TTL VALUES FOR ZA1

Rank	*TTL*	*Packet Count*	*% of total*	*Initial TTL*
1	111	25,771,844	78.57	128
2	50	3,575,563	10.90	60 or 64
3	236	920,462	2.81	255
4	234	864,950	2.64	255
5	232	434,480	1.32	255
6	46	359,082	1.09	60 or 64
7	237	111,038	0.34	255
8	242	82,377	0.25	255
9	62	78,255	0.24	60 or 64
10	47	71,969	0.22	60 or 64
	Total	32,270,020	% of total	98.39%

A. Source IP and TTL

An analysis of the observed source addresses shows that a single address (217.168.137.25) is observed at a level in excess of an order of magnitude more than the other top sources. Table I lists the traffic for the top 10 observed sources, which constitute 17.74% of the overall traffic. This indicates that the IP address was targeted from the beginning of the attack, and the varying TTL values observed further show a strong likelihood that more than one host was being used to spoof packets with this source address. The TTL values that were found in packets using the top IP address could indicate three different attacking hosts or one host with rerouted packets. As shown in the Table I, there are only two IP addresses where more than a single TTL value was observed. This is indicative of multiple participants spoofing the address, or minor routing changes having occurred during the attack. Further investigation into the temporal overlap is discussed in future work. Taking a look at the IP addresses 63.251.20.99, it can be seen that there is a distinct difference between the observed TTL values. Although the majority of the packets have a TTL of 111 (in common with the majority of traffic) there are some with a very high TTL value. The occurrences of the top 10 TTLs, are shown in Table II.

B. Time-to-Live values

There were a total of 64 distinct TTL values observed. The most frequent of these being 111, which could mean the attacker was using a Windows operating system (assuming the TTL is not spoofed) as Windows sets the initial TTL to 128. This is a similar result to [2] and may indicate a botnet being used or one host attacking multiple victims.

C. TTL Groups

Based on the top 10 TTL values shown in Table II, the IP addresses for which two or more TTLs were observed were isolated. This resulted in 4,679 IP addresses out of the 56,273 IP addresses seen, comprising just over 8% of the source addresses observed. TTL groupings were found by looking at a group and determining how many IP addresses only used those TTLs.

There were 51 different groups of TTLs found, the top 10 of which are shown in Table III. The most frequent being TTL values of 234 and 236 with 3,207 IP addresses observed using only these. Although not shown in the table the largest group included 6 out of the top 10 TTLs (62,111,232,234,236,237), however this was observed with only four IP addresses. The number of distinct TTL values observed within a group (all claiming to be from a single IP source address) is strongly indicative of multiple hosts being involved in generating the attack traffic. While the data shows that multiple hosts are unlikely involved it's difficult to determine with any certainty as to the exact number, given the vagaries of internet routing, but could indicate the number of attacking hosts.

As such first ranked TTL group in Table III could indicate that two hosts were possibly attacking 3207 different IP addresses (the spoofed source address being that of the target of the amplification attack). It could also indicate that the hosts attacking the 3207 IP addresses were using a DDoS tool that set the default TTL to 255, which means there could be more than two attacking hosts. By extension given similar routing topologies there could be two groups of hosts generating the spoofed traffic.

TABLE III. TOP 10 TTL RANGES IN ZA1

Rank	*TTL group*	*Unique IP Count*	*% of total*
1	234, 36	3207	68.54
2	232, 236	245	5.24
3	111, 236	232	4.96
4	232, 234, 236	201	4.30
5	111, 234	116	3.55
6	111, 234, 236	97	2.07
7	232, 234	72	1.54
8	234, 236, 237	72	1.54
9	236, 237	54	1.15
10	62, 111	45	0.96
Total	4341	% of total	92.78%

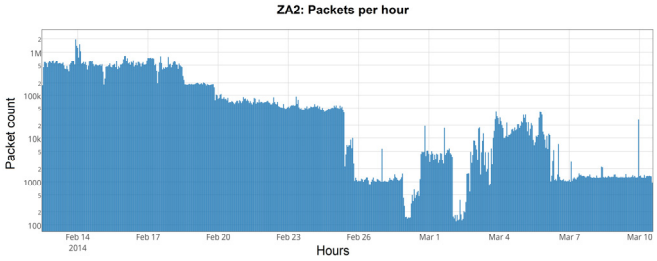

Figure 4. Packets per hour for ZA2

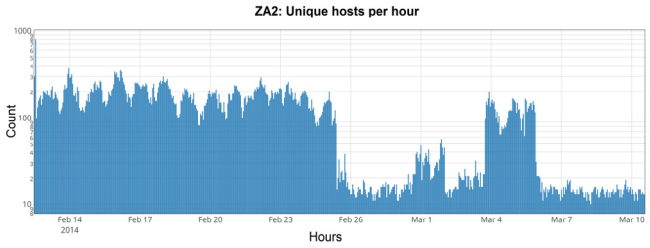

Figure 5. Unique hosts per hour for ZA2

V. ZA2 ANALYSIS

This section presents results of the analysis conducted on the ZA2 dataset. The dataset, which spans a shorter overall time period than the ZA1 set, contains nearly three times the volume of traffic, and shows sustained attack traffic over the period. As noted in Section 3.1, this merges attack traffic across a number of hosts within a /27 net block. The volume of the observed traffic is shown in Figure 4; however this lacks the clear break in attacks as seen previously in Figure 2. This attack saw a peak packet per hour rate of around 2 million, which is significantly larger than the peak rate of ZA1 (although it is acknowledged that there are a larger number of targets in this sample). Figure 5 shows a similar diurnal pattern as seen in Figure 3. Another similarity between the two unique source hosts per hour plots is the considerably high packet count at the start of the capture.

TABLE IV. TOP 10 IP ADDRESSES FROM ZA2

Rank	*IP address*	*Count*	*% of total*	*TTL*
1	217.168.137.25	18,565,847	18.01	47 (9.67%) 51 (87.98%)
2	162.218.54.28	3,158,997	3.07	232 (6.18%) 233 (7.93%) 234 (69.82%) 235 (2.29%) 236 (7.37%) 238 (6.41%)
3	192.64.169.29	2,322,018	2.25	234 (8.26%) 235 (9.02%) 236 (73.58%) 237 (0.87%) 243 (0.41%)
4	178.32.140.23	1,820,792	1.77	233 (0.37%) 235 (9.60%) 236 (66.99%) 237 (4.25%) 238 (14.65%)
				243 (0.84%)
5	198.50.180.205	1,495,278	1.45	232 (31.15%) 233(11.37%) 235 (2.51%) 236 (54.86%) 238 (0.10%)
6	37.187.77.125	1,210,377	1.17	235 (77.27%) 236 (8.34%) 237 (2.95%) 238 (11.26%)
7	178.32.137.207	825,674	0.80	232 (0.38%) 233 (6.22%) 235 (19.09%) 236 (65.16%) 237 (4.28%) 243 (1.43%)
8	94.23.19.43	751,176	0.73	233 (3.31%) 235 (35.45%) 236 (19.26%) 237 (7.38%) 243 (23.16%)
9	109.163.224.34	682,706	0.66	236 (57.45%) 237 (7.19%) 238 (34.68%) 64 (0.66%)
10	198.27.74.181	677,972	0.66	236 (43.53%) 233 (14.69%) 232 (2.36%) 234 (19.20) 235 (20.22%)
	Total	31,510,837	% of total	30.58%

A. *Source IP and TTL*

As shown in Table 4, which lists the traffic for the top 10 observed sources, there is one IP address (217.168.137.25) that is observed at a level in excess of an order of magnitude more than the other top sources. This address also appears as the top IP address in the ZA1 dataset was also observed with a high count on two or more NTP servers around the world around the time period [1], [9], [10]. The TTL values observed for (spoofed) packets originating from 217.168.137.25 were 47, 51 and 48, which are similar TTL values for this IP address in ZA1. This is indicative of multiple participants spoofing the address; minor routing occurring during the attack or the attackers used a similar DDoS tool. Most importantly it shows the exploitation of multiple servers in the amplification attacks against targets.

Unlike the ZA1 dataset where two of the top 10 source addresses used more than one TTL, the ZA2 dataset shows all top 10 addresses using more than two TTL values. This strongly supports the supposition that more than one attacker was used to attack a victim and one victim attacked multiple hosts.

B. *Time-to-Live values*

There were a total of 64 distinct TTL values observed. The most frequent of these being 111, which could mean the attacker was using a Windows operating system (assuming the initial TTL is not spoofed) as Windows sets the initial TTL to 128. This is a similar result to [2] and may indicate a botnet being used or one host attacking multiple victims.

TABLE V. TOP 10 TTL VALUES FOR ZA2

Rank	*TTL*	*Packet Count*	*% of total*	*Initial TTL*
1	236	23,509,039	22.81	255
2	235	17,009,527	16.50	255
3	51	16,778,624	16.28	60 or 64
4	237	13,946,335	13.53	255
5	232	4,054,193	3.93	255
6	234	3,893,500	3.78	255
7	238	2,755,487	2.67	255
8	243	2,451,201	238	255
9	64	2,232,754	2.17	100/128?
10	233	2,152,300	2.08	255
	Total	88,782,960	% of total	86.15%

TABLE VI. TOP 10 TTL RANGES IN ZA2

Rank	*TTL group*	*Unique IP Count*	*% of total*
1	235, 237	3440	38.99
2	233, 237	244	2.77
3	233, 235, 237	167	1.89
4	234, 237	137	1.55
5	236, 237	131	1.48
6	234, 235, 237	93	1.05
7	232, 234	88	1.00
8	237, 64	88	1.00
9	235 ,236, 237	69	0.78
10	235, 237, 238	60	0.68
Total	4517	% of total	51.20%

C. TTL Groups

From the top 10 TTL values seen (shown in Table V), the IP addresses which used two or more TTLs were found. This resulted in 8,823 IP addresses out of the 38,634 IP addresses seen. There were 143 different groups of TTLs found, the top 10 of which are shown in Table VI. The most frequent being 235 and 237 with 3440 IP addresses observed using only these. Although not shown in the table the largest group of top 10 TTLs included of 9 out of the top 10 TTLs (232,233,234,235,236,237,238,51,64) however, only one (spoofed) IP address was observed to be part of this grouping. This again illustrates the strong evidence towards multiple sources for the spoofed traffic.

VI. CONCLUSION

This paper has presented initial exploratory analysis of the IPv4 Time-to-Live values observed in two NTP based DDoS attack datasets. Multiple source hosts were found to be attacking one victim system, though the exploitation of amplification. This was determined due to the numerous source addresses using multiple TTL values. Since many of the TTL values observed are >230, it could mean that the attacking hosts are using the same initial TTL of 255. This was confirmed by reviewing the source of several common NTP DDos tools, which explicitly set the TTL field of the generated packets to the maximum value.

We were also able to infer the number attackers (or attackers sharing common routing paths) targeting a certain victim, by finding the TTL used for each source address. In addition, the results show that these attacks utilise more than one vulnerable NTP server during an attack.

A. It was found that the main targets of these attacks are gaming related servers, which is an expected result as gaming servers are a major target, particularly in DDoS attacks focusing on bandwidth exhaustion. Future Work

The next steps of this work will include further analysis using the IP datagram and UDP datagram lengths to further characterise NTP DDoS attacks. An analysis of the packet contents will also be carried out as well as looking at the source ports used by the packets and find their uses, which should expectedly be game related.

REFERENCES

[1] BG.net. (2014). *NTP reflection attack - a vulnerability in implementations of NTP*. Available: http://bg.net.ua/content/ntp-reflection-attack-uyazvimost-v-realizatsiyakh-protokola-ntp

[2] Czyz, Jakub, Michael Kallitsis, Manaf Gharaibeh, Christos Papadopoulos, Michael Bailey, and Manish Karir "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks." *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014.

[3] Higgins, Kelly Jackson. "Attackers Wage Network Time Protocol-Based DDoS Attacks. News Article." (2013).

[4] Mimoso, M. "*Dramatic drop in vulnerable NTP servers used in DDoS attacks*. News Article*."* (2014).

[5] Mimoso, M. "*SNMP based DDoS attacks Spoofs Google public DNS server*. News Article." (2014).

[6] Networks, A. (2014, October). *Arbor Networks' ATLAS Data Shows Reflection DDoS Attacks Continue to be Significant in Q3 2014*. [Online] Available: http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5283-arbor-networks-atlas-data-shows-reflection-ddos-attacks-continue-to-be-significant-in-q3-2014 (Accessed 24 October 2014)

[7] NSFOCUS. (2014, February). *NTP amplification attacks are one the rise? (Part 1)* [Online] Available: http://nsfocusblog.com/2014/02/04/ntp-amplification-attacks-are-on-the-rise-part-1 (Accessed 3 March 2014)

[8] Prince, Matthew. "Technical details behind a 400Gbps NTP amplification DDoS attack." *Cloudflare, Inc* 13 (2014)

[9] StPaddy. (2014, February 16). *VMWare esxi 3.x - High Bandwidth* [Online]. Available: http://community.spiceworks.com/topic/445704-vmware-esxi-3-x-high-bandwidth (Accessed 3 March 2014)

[10] University, T. (2014, February 16). *IP traffic school* [Online]. Available: http://traffic.ttu.edu.tw/gigaflow/extipflow.php?start=2014-02-16&end=2014-02-16&OrderBy=stin (Accessed March 2014)